Federal Computer Incident Response Capability

The FedCIRC Bits & Bytes

A monthly newsletter for Information System Security Managers/Officers & System Administrators

October 1, 2000 Volume I, Issue 4

Notes from the Director

The Times, They are a Changin'

Fiscal year 2001 promises, with absolute certainty, to be more challenging than ever before. More requirements and less funding seems to be the rule rather than the exception and for that reason, the information technology (IT) security professional will have to apply exceptional planning and intellect to counter the growing threats. System life-cycle support must now reflect a non-negotiable bonding of systems engineering and security requirements. One may not exist without the other or organizational IT budgets will likely suffer. Configuration management processes must now form a cornerstone on which system integration and implementation processes revolve. The mindset of "anything goes out of operational necessity" is quickly being overcome by the reality that operational needs can only be reliably met in an identifiable and controlled environment. Risks must be mitigated with respect to the prevailing threats. Sadly, these requirements have been in place for well over a decade, yet the IT security professional has had too little power, miniscule budgets (if any) and insufficient influence within the organization to enact the necessary changes. On a lighter note, I see changes coming as senior managers become more sensitized to the associated issues and more committed to the protection of critical infrastructure networks and components. It isn't going to happen overnight, but clearly changes are coming.

Upcoming Event

The **Information Technology Security Innovations Conference,** sponsored by Federal Computer Incident Response Capability (FedCIRC), will be held November 7-8, 2000 at the Inn and Conference Center of University of Maryland University College, College Park, MD. The conference theme focuses on the current challenges and threats facing the Federal IT security professional and will introduce new developments in security solutions. Guest speakers will address a variety of associated topics and conduct expert panels discussing "hacker profiling," "web security practices," "Federal security initiatives," "current status of agency security postures" and "best security practices." Approximately 40 vendors will be on hand displaying the latest technology solutions. Conference will run each day from 8:30am to 4:00pm. There will be shuttle bus service from the College Park Metro in the morning and service in the afternoon. Parking is free at the conference center. This is one you don't want to miss. For more information and registration go to http://www.fedpage.com/fedcirc.

Weaknesses in Virus Checkers

by: NIST (ITL Bulletin, 6/2000)

A related problem exists with virus checkers. Here, the attacker does not need to wait for a new attack to be released, but can simply create a new virus that won't be detected. The problem is that virus detection software detects only the viruses that have been previously analyzed and added to the software's database. Such software has great difficulty in detecting never-before-seen viruses. A hacker who wishes to penetrate a particular company can write a virus specifically for that organization. By testing the virus beforehand on the handful of popular virus-checking programs, the hacker can guarantee that the virus will enter the organization undetected. The hacker then sends an innocuous e-mail and the malicious code will likely be executed within the target organization.

FedCIRC Quarterly Summary

Each quarter we issue the FedCIRC Summary to draw attention to the types of attacks that are being reported, as well as other noteworthy incident and vulnerability information. The summary includes pointers to sources of information for dealing with the respective problems. FedCIRC summaries are available at:
http://www2.fedcirc.gov/summaries/

Recent Activity

FedCIRC has published information on a vulnerability in rpc.statd on Linux systems, several ActiveX controls, vulnerabilities in Outlook and Outlook Express, security considerations for using chat software, hidden file extensions, and vulnerabilities in many FTP daemons.

We began receiving reports of sites being root compromised via a recently discovered vulnerability in rpc.statd. These issues are described in FedCIRC Advisory FA-2000-17. Reports indicate intruders were performing widespread scanning for this vulnerability and using toolkits to automate the compromise of vulnerable machines.

FedCIRC continues to receive regular reports of intruders probing for and exploiting vulnerabilities in FTP server implementations. Sites are strongly encouraged to follow the advice contained in FA-2000-13 to protect FTP enabled servers.

ActiveX Control Vulnerabilities

Exploitations of a vulnerability in the Scriptlet.Typelib ActiveX control are discussed in CERT Incident Note IN-2000-06. This vulnerability allows local files to be created or modified and is used in viruses such as Bubbleboy and kak. For more information, go to:
http://www.cert.org/incident_notes/IN-2000-06.html

Additionally, information relating to serious vulnerability in the HHCtrl ActiveX control was published in FedCIRC Advisory FA-2000-12. This vulnerability may allow remote intruders to execute arbitrary code.

Exploitation of Hidden File Extensions

Attackers have used a number of malicious programs to exploit the default behavior of Windows operating systems to hide file extensions from the user. This behavior can be used to trick users into executing malicious code by making a file appear to be something it is not. CERT Incident Note IN-2000-07, Exploitation of Hidden File Extensions explains this exploit in greater detail at:
http://www.cert.org/incident_notes/IN-2000-07.html

A vulnerability in Microsoft Outlook and Outlook Express that can allow a remote attacker to read certain types of files on the user's machine is detailed in FedCIRC Advisory FA-2000-14.

Chat Clients and Network Security

CERT Incident Note IN-2000-08 outlines the security issues inherent in the use of chat client software. We have published this information in response to inquiries relating to the risks this type of software poses to an organization.
http://www.cert.org/incident_notes/IN-2000-08.html

Establishing a Computer Security Incident Response Plan

Part I of this article was published in the September Bits & Bytes Newsletter.

A major portion of any set of procedures is identifying who will be performing these procedures. The plan must describe the makeup and duties of the Computer Security Incident Response Team (CSIRT). The CSIRT is composed of a core group of responders who is involved in all incidents and a group of platform and system specialists whose participation on the team will be required for each incident. The core group should include the Information Technology Security Professional Manager as the CSIRT leader, the Legal Department, Human Resources, and someone with an investigative/forensics background. This does not exclude an agency from including additional personnel in the core group of the CSIRT. The CSIRT members will need to know who they are required to contact during an incident investigation. At a minimum, the Federal Computer Incident Response Capability should be contacted for informational reasons as well as for assistance in combating the incident.

Calendar of Events

Computer Security Incident Handling for Technical Staff (Advanced)
Date: Oct 16-20, 2000
Location: Carnegie Mellon Univ, Software Engineering Institute (CERT/CC), Pittsburgh, PA
POC: 412-268-7702
http://www.cmu.edu/products/courses/csih-advanced.html

Introduction to Computer and Network Security
Date: Oct 31- Nov 1 or Nov 11-12, 2000
Location: varies
POC: Computer Security Institute, 415-905-2626
http://www.gocsi.com/wkshop.shtml

Information Technology Security Innovations Conference
Date: Nov 7-8, 2000
Location: UMUC, Conference Center, College Park, MD
POC: FedCIRC (800) 878-2940 x234
http://www.fedpage.com/fedcirc

Windows NT Security
Date: Nov 11-12, 2000
Location: Chicago, IL
POC: Computer Security Institute, 415-905-2626
http://www.gocsi.com/wkshop.shtml

Managing Computer Security Incident Response Teams (CSIRTs)
Date: Nov 14-16, 2000
Location: Carnegie Mellon Univ, Software Engineering Institute (CERT/CC), Arlington, VA
POC: 412-268-7702
http://www.sei.cmu.edu/products/courses/managing-csirts.html

Secure Migration to Windows 2000
Date: Nov 16-18, 2000
Location: varies
POC: Computer Security Institute, 415-905-2626
http://www.gocsi.com/wkshop.shtml

Viruses, Worms, & Trojans in the Wild

W32.ExploreZip.F.Worm: Also known as *W32/ExploreZip.worm trojan, Worm.ExploreZip*

JS/VBS.LostSoul.Worm: Also known as *NETWORK/OUTLOOK.FakeHoax, JS/Wobble.worm*

VBS/Quatro.a: Also known as *VBS.Disabled.Worm, update.vbs*

The FedCIRC Bits & Bytes Newsletter

Director
David Jarrell
Project Manager for Marketing/Outreach
Connie Oden
Editor
Diane Queen
Contributing Editors
David Adler
Kenneth Grossman
Charmayne Parks
Corliss McCain

We welcome your input! To submit your related articles and notices for future issues, please contact FedCIRC at 202-708-5060. Deadline for submissions is the 15th of each month. Articles may be edited for length and content. Back issues of this newsletter can be found on the FedCIRC website www.fedcirc.gov/docs.html

FedCIRC is sponsored by the Federal CIO Council and is operated by the General Services Administration/Federal Technology Service